REMARKS

Reconsideration and allowance of the application are respectfully requested in light of the above amendments and the following remarks.

Claims 1, 9, and 14 have been amended, claims 7, 10, and 13 have been cancelled, and claims 15 and 16 have been newly added. Support for the amendments is provided at least in the original claims and paragraph [0044] of the specification.

Claims 8 and 9 stand withdrawn for being directed toward non-elected subject matter.

Claims 1-7 and 10-14 were rejected, under 35 USC §103(a), as being unpatentable over Lee et al. (US 2004/0242228) in view of Eaton et al. (US 6,888,811). To the extent these rejections may be deemed applicable to the amended claims, the Applicants respectfully traverse based on the points set forth below.

Claim 1 defines a centralized management authentication apparatus that notifies only one wireless network of a wireless terminal's authentication information each time the wireless terminal accesses the one wireless network or at a fixed interval. By notifying the wireless network in this fashion, the claimed invention provides an advantage of making it possible to change an encryption key of a wireless channel, which is included in the wireless terminal's authentication information, so as to

enhance security of the channel (see the published specification ¶ [0044]).

The Applicants respectfully submit that Lee and Eaton, considered alone or together, fail to teach or suggest the claimed feature of an authentication apparatus that notifies only one wireless network of a wireless terminal's authentication information each time the wireless terminal accesses the one wireless network or at a fixed interval. Instead, Lee discloses that when a wireless terminal becomes associated with an access point (i.e., wireless network), an authentication server (AS) generates a communication encryption key for each neighboring access point (AP), based on information of the association, and communicates both the key and association information to each neighboring access point (see Lee ¶¶ [0040 and 0102]). As a result, each neighboring access point stands ready to communicate with the wireless terminal should the terminal roam into the access point (see ¶ [0102], last sentence). Eaton does not disclose an authentication server and, thus, does not supplement the teachings of Lee in any way relevant to the above-noted claimed subject matter.

Accordingly, the Applicants respectfully submit that Lee and Eaton, considered individually or in combination, do not disclose or render obvious the subject matter defined by claim 1.

To promote a better understanding of the differences between the claimed invention and the applied references, the Applicants provide the following additional remarks.

According to present claim 1, a centralized management authentication apparatus manages information of a current location of a wireless terminal apparatus and service area information of each of a plurality of wireless networks, notifyies only at least one of the wireless networks that provides communication services in a peripheral area of the current location of the wireless terminal apparatus of authentication information required for authentication of the wireless terminal apparatus before the wireless terminal apparatus moves to the at least one of the wireless networks, and, more particularly, performs notification to the at least one of the wireless networks each time the wireless terminal apparatus accesses the at least one of the wireless networks or at fixed intervals. According to these features, an advantage is provided of making it possible to change an encryption key of a wireless channel included in the authentication information and enhance security.

In contrast, Lee discloses a service roaming method for a fast and secure wireless network. According to this method, an authentication server transmits proactive keys needed for roaming

to access points neighboring one that has associated with a wireless terminal. When the wireless terminal moves to one of the neighboring access points, a re-association is carried out between the wireless terminal and the neighboring access point using the already provided proactive key. Eaton discloses a portable device that communicates with a short-range wireless local area network and a wide area communication system. The portable device receives location data from the short-range wireless local area network and generates a location-sensitive information request to the wide area communication system that includes the location data received from the short range wireless local area network.

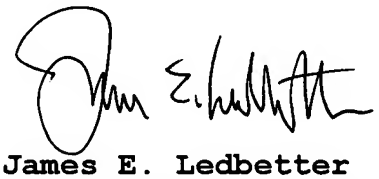
From the above discussions of Lee et al. nor Eaton et al., it is apparent that these references, alone or together, fail to disclose or suggest the features of the invention of present claim 1.

Independent claims 14-16 similarly recite the above-mentioned feature distinguishing apparatus claim 1 from the applied references, although claim 14 does so with respect to a method. Therefore, allowance of claims 1 and 14-16 and all claims dependent therefrom is warranted.

In view of the above, it is submitted that this application is in condition for allowance and a notice to that effect is respectfully solicited.

If any issues remain which may best be resolved through a telephone communication, the Examiner is requested to telephone the undersigned at the local Washington, D.C. telephone number listed below.

Respectfully submitted,



Date: March 30, 2007
JEL/DWW/att

James E. Ledbetter
Registration No. 28,732

Attorney Docket No. L9289.05164
STEVENS DAVIS, MILLER & MOSHER, L.L.P.
1615 L Street, N.W., Suite 850
P.O. Box 34387
Washington, D.C. 20043-4387
Telephone: (202) 785-0100
Facsimile: (202) 408-5200